UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/797,773	03/09/2004	Mark Ammar Rayes	50325-0865	4164

29989 7590 11/28/2008

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
SHAIFER HARRIMAN, DANT B	
ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
11/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/797,773	RAYES ET AL.	
	Examiner	Art Unit	
	DANT B. SHAIFER HARRIMAN	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 July 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 - 14 & 16 - 20 & 24 - 26 & 28 - 44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 - 14 & 16 - 20 & 24 - 26 & 28 - 44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Status of the instant application:

- Claim 15 & 21 – 23 & 27 have been cancelled in the instant application.
- Claims 43, 44 are new in the instant application.
- Claims 2, 8, 11, 13 are original in the instant application.
- Claims 1, 3 - 7 & 9, 10, 14, 16 - 20, 24 - 26, 28 - 37, 39 - 42 are currently amended in the instant application.
- Claims 12, 38 are previously presented in the instant application.

Response to Arguments

- Applicants arguments/remarks and amendments filed 07/14/2008 have been fully considered and are not persuasive, please see the examiners response to applicant arguments and office action below.

Examiners response to applicant's arguments:

Applicant states: "The Examiner also agreed to provide, in writing, his explanation of the suggestion and motivation to combine the references in the next office action."

- The examiner respectfully disagrees with applicant's logic and reasoning, the examiner points to 35 USC 103a rejections in the office action below.

Applicant states: "Neither of the cited references teaches or suggests "determining whether a malicious act caused the security event," as recited in Claim 14. "

- The examiner respectfully disagrees with applicants logic and reasoning, the examiner points to Col. 5, lines 54 - 65, Col. 11, lines 62 - 63, Col. 12, lines 4 - 9, the examiner notes that a the security event (i.e. the device being not authenticated) and the determining whether a malicious act caused the security event (i.e. checking the pre-stored authentication information with the devices presented authentication information).

- In addition the Examiner notes the amended claim 1 indicates "wherein the security event is an event that indicates at lest one of: a possible denial of service attack, possible IP address spooking, extraneous requests for network address, and possible MAC address spoofing". Thomsen teaches methods of intrusive access is spoofing, and provides examples of spoofing in col. 3, line 18 through col. 4, line 64. The invention is directed to method of preventing damage from possible spoofing or unauthorized access see col. 5, lines 9-18. Thomsen places devices that are not authenticated in an un-trusted subnet. Thomsen also prevents spoofing in col. 10, lines 25-61 if a device has remained if they have failed to re-authenticate for a period of time, this prevents a device from spoofing an IP address. Therefore since Applicant's disclosure describe a security event as spoofing, the rejection applied below is correct because Thomsen prevents damage caused by spoofing or un-authenticated devices.

Applicant states: "The Office Action alleges that an authentication failure is a "security event" within the meaning of Claim 1. However, the Office Action does not specifically allege any element of Thomsen that corresponds to the "malicious act" of Claim 14. Nor does the Office Action specifically allege any step of Thomsen that corresponds to "determining whether a malicious act caused the security event." "

- The examiner respectfully disagrees with applicants logic and reasoning, the examiner points to Col. 5, lines 54 - 65, Col. 11, lines 62 - 63, Col. 12, lines 4 – 9 of Thomsen, the examiner notes that a the security event (i.e. the device being not authenticated) and the determining whether a malicious act caused the security event (i.e. checking the pre-stored authentication information with the devices presented authentication information)

Applicant states: "This interpretation is unsupported and conflicts with the ordinary meaning of "malicious." An authentication failure may or may not have been caused by a malicious act. For example, it may instead be caused by a benign user error, such as a forgotten password. "

- The examiner respectfully disagrees with applicants logic and reasoning, the examiner points to Col. 5, lines 54 - 65, Col. 11, lines 62 - 63, Col. 12, lines 4 – 9 of Thomsen, the examiner further notes that in order to give the claim limitation "malicious" a fair interpretation, the applicant must also consider the event that a malicious user who obtains the any users authentication information, meaning this particular user isn't a known malicious user that commits malicious acts, now when a malicious user obtains a valid users authentication information and masquerades as a valid user, by inputting the users authentication information, and gaining access to a secured area, with the intent to commit malicious acts.

Applicant states: "Furthermore, Claim 14 would not make sense if an authentication failure is both a security event and a malicious act. Simple word-substitution illustrates the problem--a process would not "determine[e] whether a[n] [authentication failure] caused the [authentication failure]." "

- The examiner respectfully disagrees with applicants logic and reasoning, the examiner points to Col. 5, lines 54 - 65, Col. 11, lines 62 - 63, Col. 12, lines 4 – 9 of Thomsen, the examiner notes that the determining whether a malicious act caused the security event (i.e. checking the pre-stored authentication information with the devices presented authentication information.

Applicant states: "*Thus, Thomsen's* authentication failure does not teach or suggest a "malicious act." Nor does *Thomsen* in any way teach or suggest "determining whether a malicious act caused the security event" within the meaning of Claim 14. "

- The examiner respectfully disagrees with applicants logic and reasoning, the examiner points to Col. 5, lines 54 - 65, Col. 11, lines 62 - 63, Col. 12, lines 4 – 9 of Thomsen, the examiner notes that a the security event (i.e. the device being not authenticated) and the determining whether a malicious act caused the security event (i.e. checking the pre-stored authentication information with the devices presented authentication information)

Applicant states: "This element is also missing from *Renda.* "

- The examiner respectfully disagrees with applicant's logic and reasoning, the examiner points to the examiners previous logic and reasoning above with regard to Thompsen.

Applicant states: "Also, neither of the cited references teaches or suggests a step of "if a malicious act caused the security event, then providing information about the security event or malicious act to a security decision controller," as recited in Claim 14. "

- The examiner respectfully disagrees with applicants logic and reasoning, the examiner points to (Col. 5, lines 54 - 65, Col. 11, lines 62 - 63, Col. 12, lines 4 -

9, the examiner notes that the security event is interpreted as if the authentication of the device fails);

Applicant states: "Not only do these passages fail to describe a malicious act that caused this alleged security event, these passages fail to disclose that one may forward information to a security decision controller about the security event if the security event was caused by a malicious act. "

- The examiner respectfully disagrees with applicants logic and reasoning, the examiner points to Col. 5, lines 54 - 65, Col. 11, lines 62 - 63, Col. 12, lines 4 – 9 of Thomsen, the examiner notes that the determining whether a malicious act caused the security event (i.e. checking the pre-stored authentication information with the devices presented authentication information, the validation of the comparing of the credentials is the determining of a malicious act, the outcome of the validation is then sent to DHCP (i.e. Dynamic Host Configuration protocol) server (i.e. security decision controller).

Applicant states: "This element is also missing from *Renda.* "

- The examiner respectfully disagrees with applicant's logic and reasoning, the examiner points to the examiners previous logic and reasoning above with regard to Thompsen.

Applicant states: "Furthermore, neither of the cited references teaches or suggests "if a malicious act did not cause the security event, then removing the user from the elevated risk group," as recited in Claim 14."

- The examiner respectfully disagrees with applicants logic and reasoning, the examiner points specifically to Col. 5, lines 62 – 65, the examiner notes that the requesting device is put into a subnet of IP (i.e. internet protocol) addresses that associated with un-trusted IP addresses, then when the requesting device is

authenticated, the requesting device to removed from the un-trusted IP addresses subnet and is assigned to a subnet of trusted IP addresses.

Applicant states: "As mentioned previously, these passages of *Thomsen* disclose only that one may place a device on an untrusted subnet in the event of an authentication failure. The passages say nothing about, after placing a device on an untrusted subnet, subsequently returning the device to a trusted subnet if the authentication failure was not caused by a malicious act. "

- The examiner respectfully disagrees with applicants logic and reasoning, the examiner points to Col. 5, lines 62 – 65, the examiner notes that the requesting device is put into a subnet of IP (i.e. internet protocol) addresses that associated with un-trusted IP addresses, then when the requesting device is authenticated, the requesting device to removed from the un-trusted IP addresses subnet and is assigned to a subnet of trusted IP addresses

Applicant states: "Thus, *Thomsen's* authentication failure does not teach or suggest the security event of Claim 1. Nor does any other element of *Thomsen* or *Renda* teach or suggest the security event of Claim 1. "

- The examiner respectfully disagrees with applicant's logic and reasoning, the examiner points to Col. 2, lines 52 – 67 & Col. 3, lines 1 – 67 & Col. 4, lines 1 – 67 & Col. 4, lines 1 – 5, the examiner notes specifically, Col. 4, lines 18 – 28 & Col. 8, lines 12 – 14, the examiner notes that one way of spoofing is for the malicious user to obtain a static IP address (i.e. an IP address that doesn't change), which by passes the DHCP server, now with this said, the client device # 320 does acquire a static IP address, this indicates that the reference of Thomsen does in fact prevent IP address spoofing.

Applicant states: "Neither of the cited references teaches or suggests causing such a device to subsequently receive a second network address."

- The examiner respectfully disagrees with applicants logic and reasoning, the examiner points to Col. 5, lines 62 – 65, the examiner notes that the requesting device is put into a subnet of IP (i.e. internet protocol) addresses that associated with un-trusted IP addresses (i.e. first address), then when the requesting device is authenticated, the requesting device to removed from the un-trusted IP addresses subnet and is assigned to a subnet of trusted IP addresses (i.e. second address)

Applicant states: "The Office Action alleges that *Thomsen* teaches such a step in col. 5, lines 54-65, col. 11, lines 62-63, and col. 12, lines 4-9. The Office Action is in error. Although these passages of *Thomsen* disclose that one may place a device on an untrusted subnet in the event of an authentication failure, the device placed on the untrusted subnet cannot be considered to have been assigned a "second network address" because the device never had a "first network address assigned from a first subset of addresses within a first specified pool associated with normal network users." "

- The examiner respectfully disagrees with applicants logic and reasoning, the examiner points to Col. 5, lines 62 – 65, the examiner notes that the requesting device is put into a subnet of IP (i.e. internet protocol) addresses that associated with un-trusted IP addresses (i.e. first address), then when the requesting device is authenticated, the requesting device to removed from the un-trusted IP addresses subnet and is assigned to a subnet of trusted IP addresses (i.e. second address)

Applicant states: "In fact, since *Thomsen's* device has not been authenticated on the network, it would have been impossible for *Thomsen's* device to have a "first network address assigned from a first subset of addresses within a first specified pool associated with normal network users." Thus, it could not then be assigned a "second network address." "

- The examiner respectfully disagrees with applicants logic and reasoning, the examiner points to Col. 5, lines 62 – 65, the examiner notes that the requesting device is put into a subnet of IP (i.e. internet protocol) addresses that associated with un-trusted IP addresses (i.e. first address), then when the requesting device is authenticated, the requesting device to removed from the un-trusted IP

addresses subnet and is assigned to a subnet of trusted IP addresses (i.e. second address)

Applicant states: "For the same reasons, *Thomsen* fails to disclose a security event caused by a network device "having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users." "

- The examiner respectfully disagrees with applicants logic and reasoning, the examiner points to Col. 5, lines 62 – 65, the examiner notes that the requesting device is put into a subnet of IP (i.e. internet protocol) addresses that associated with un-trusted IP addresses (i.e. first address), then when the requesting device is authenticated, the requesting device to removed from the un-trusted IP addresses subnet and is assigned to a subnet of trusted IP addresses (i.e. second address)

Applicant states: "*Thomsen* further fails to disclose a security event within the meaning of Claim 1, because the authentication failure does not come from a network device having said first network address."

- The examiner respectfully disagrees with applicants logic and reasoning, the examiner points to Col. 5, lines 62 – 65, the examiner notes that the requesting device is put into a subnet of IP (i.e. internet protocol) addresses that associated with un-trusted IP addresses (i.e. first address), then when the requesting device is authenticated, the requesting device to removed from the un-trusted IP addresses subnet and is assigned to a subnet of trusted IP addresses (i.e. second address)

Applicant states: "The Office Action alleges that such a step is disclosed in *Thomsen* at col. 8, lines 12-14 and col. 10, lines 62-64. The Office Action is in error. These passages say nothing about "resetting a port." "

- The examiner respectfully disagrees with applicants logic and reasoning, the examiner points to Col. 8, lines 12 – 14, Col. 10, lines 62 – 64, the examiner notes that to one of ordinary skill in the art, there are many ways to "reset a port," one way is that a new device with a different IP address start to communicate with the port, that previously had another device with a different IP address communicating information to the same port.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim(s) 1- 14 & 16 – 20 & 24 – 26 & 28 - 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomsen (US Patent NO. 7194004 B1) in view of Renda et al. (US Patent NO. 7127524 B1)

Thomsen discloses:

1. A method, comprising the computer-implemented steps of:

- in response to the security event, causing the network device to acquire a new network address that is selected

from a second subset of addresses within a second specified pool associated with suspected malicious network users (Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner notes that the security event is interpreted as if the authentication of the device fails);

wherein the security event is an event that indicates at least one of:

- a possible denial of service attack, possible IP address spoofing extraneous requests for network addresses, and possible MAC address spoofing(Col. 2, lines 52 – 67 & Col. 3, lines 1 – 67 & Col. 4, lines 1 – 67 & Col. 4, lines 1 – 5, the examiner notes specifically, Col. 4, lines 18 – 28 & Col. 8, lines 12 – 14, the examiner notes that one way of spoofing is for the malicious user to obtain a static IP address (i.e. an IP address that doesn't change), which by passes the DHCP server, now with this said, the client device # 320 does acquire a static IP address, this indicates that the reference of Thomsen does in fact prevent IP address spoofing.);

wherein

- the second subset of addresses is different from the first subset of addresses(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner notes that un-trusted and trusted IP addresses are different); and

- configuring one or more security restrictions with respect to the selected new network address(Col. 11, lines 23 – 34, Col. 11, lines 51 – 56).

3. A method as recited in Claim 44, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein the step of causing the network device to acquire the second network address comprises resetting a port that is coupled to the network device to prompt a user to command the network device to request a new network address using DHCP(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address).

4. A method as recited in Claim 44, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein the step of causing the network device to acquire the second network address comprises issuing a DHCP FORCE_RENEW message to the network device(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 11, lines 56 - 60, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address).

5. A method as recited in Claim 44, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein the step of causing the network device to acquire the second network address comprises prompting the network device to request a new network address using DHCP(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address).

6. A method as recited in Claim 1, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein the step of causing the network device to acquire the second network address comprises waiting for expiration of a lease for a current network address of the network device (Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 11, lines 56 - 60, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address).

7. A method as recited in Claim 1, wherein

- the step of causing the network device to acquire the second network address comprises the step of providing the network device with an IP address that is selected from a plurality of

IP addresses within a special IP subnet(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address).

8. A method as recited in Claim 7, further comprising

- the step of publishing information describing characteristics of the special IP subnet to network service providers(Col. 9, lines 36 - 38).

12. A method as recited in Claim 1, further comprising the steps of determining

- whether a malicious act caused the security event, and if not, removing the user from the second specified pool(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9).

13. A method as recited in Claim 1, further comprising

- the steps of determining whether a malicious act caused the security event, wherein a legal user action in the network is not determined to be a malicious act if the user is associated with a trusted customer of a network service provider(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9).

14. A method, comprising the computer-implemented steps of:

- in a security controller that is coupled, through a network, to a network device having a first network address assigned

from a first subset of addresses within a first specified pool associated with normal network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9):

- receiving information identifying a security event in the network(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- correlating the security event information with network user information to result in determining a network user associated with the network device that caused the security event(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- in response to receiving the information identifying the security event, placing the user in an elevated risk security group by causing the network device to acquire a second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address);

wherein

- the second subset of addresses is different from the first subset of addresses(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- configuring one or more security restrictions with respect to the selected second network address(Col. 11, lines 23 – 34, Col. 11, lines 51 – 56, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address);

- determining whether a malicious act caused the security event(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner notes that the security event is interpreted as if the authentication of the device fails);

if a malicious act caused the security event, then providing information about the security event or malicious act to a security decision controller(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner notes that the security event is interpreted as if the authentication of the device fails);

if a malicious act did not cause the security event, then removing the user from the elevated risk group(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner notes that the security event is interpreted as if the authentication of the device fails).

16. A method as recited in Claim 14, wherein causing the network device to acquire the second network address comprises the

steps of:

- re-configuring a dynamic host control protocol (DHCP) server to require said server to issue any new network address to the network device only from a specified group of network addresses that is reserved for users associated with elevated user risk(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

  and

performing any one of the steps of:

(a) resetting a port that is coupled to the network device to trigger the network device to request a new network address using DHCP();

(b) issuing a DHCP FORCE_RENEW message to the network device();

(c) prompting the network device to request a new network address using DHCP(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64); or

(d) waiting for expiration of a lease for the first network address of the network device().

18. A computer-readable storage medium carrying one or more sequences of instructions, which instructions, when executed by one or more processors, cause the one or more processors to

carry out the steps of (Col. 12, lines 43 - 59):

- in a security controller that is coupled, through a network, to a network device having first network address assigned from a first subset of addresses within a first specified pool associated with normal network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9):

- in response to the security event, causing the network device to acquire a second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner notes that the security event is interpreted as if the authentication of the device fails, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address);

  wherein

- the second subset of addresses is different from the first subset of addresses(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- and configuring one or more security restrictions with respect to the second network address(Col. 11, lines 23 – 34, Col. 11, lines 51 – 56, the examiner further notes that the examiner interprets, that the added claim limitation of,

"second network address," as the client device acquiring a new IP address).

19. An apparatus, comprising:

- in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9):

- means for, in response to the security event, causing the network device to acquire a second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner notes that the security event is interpreted as if the authentication of the device fails, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address);

wherein

- the second subset of addresses is different from the first subset of addresses(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9):

- and means for configuring one or more security restrictions with respect to the second network address(Col. 11, lines 23 – 34, Col. 11, lines 51 – 56, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address).

20. An apparatus, comprising:

- a network interface that is coupled to a data network for receiving one or more packet flows therefrom(Col. 5, lines 9 – 17, Col. 11, lines 23 – 34, the firewall or gateway is considered as a network interface that is coupled to the data network);
- a processor(Col. 12, lines 60 - 64);
- one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of(Col. 12, lines 43 - 49):
- in a security controller that is coupled, through the data network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9):
- in response to the security event, causing the network device to acquire a second network address that is selected

from a second subset of addresses within a second specified pool associated with suspected malicious network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner notes that the security event is interpreted as if the authentication of the device fails, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address);

wherein

- the second subset of addresses is different from the first subset of addresses(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9):

- and configuring one or more security restrictions with respect to the second network address(Col. 11, lines 23 – 34, Col. 11, lines 51 – 56, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address).

24. A computer-readable storage medium carrying one or more sequences of instructions, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

- in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9):

- receiving information identifying a security event in the network(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- correlating the security event information with network user information to result in determining a network user associated with the network device that caused the security event(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- in response to receiving the information identifying the security event, placing the user in an elevated risk security group by causing the network device to acquire a second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address);

wherein

- the second subset of addresses is different from the first subset of addresses(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- configuring one or more security restrictions with respect to the second network address(Col. 11, lines 23 – 34, Col. 11, lines 51 – 56, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address);

- determining whether a malicious act caused the security event(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- if a malicious act caused the security event, then providing information about the security event or malicious act to a security decision controller(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- if a malicious act did not cause the security event, then removing the user from the elevated risk group(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9).

25. An apparatus comprising

- in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9):

- means for receiving information identifying a security event in the network(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner notes that the security event is interpreted as if the authentication of the device fails);

- means for correlating the security event information with network user information to result in determining a network user associated with the network device that caused the security event(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- means for, in response to receiving the information identifying the security event, placing the user in an elevated risk security group by causing the network device to acquire a second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address);

wherein

- the second subset of addresses is different from the first subset of addresses(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- means for configuring one or more security restrictions with respect to the second network address(Col. 11, lines 23 – 34, Col. 11, lines 51 – 56, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address);

- means for determining whether a malicious act caused the security event(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- means for, if a malicious act caused the security event, then providing information about the security event or malicious act to a security decision controller(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- means for, if a malicious act did not cause the security event, then removing the user from the elevated risk group(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9).

26. An apparatus, comprising:

- a network interface that is coupled to a data network for receiving one or more packet flows therefrom(Col. 5, lines 9 – 17, Col. 11, lines 23 – 34, the firewall or gateway is considered as a network interface that is coupled to the data network to allow for packet flow to the data network);

- a processor(Col. 12, lines 60 - 64); and

- one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out(Col. 12, lines 43 - 49):

- in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9):

- receiving information identifying a security event in the network(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- correlating the security event information with network user information to result in determining a network user associated with the network device that caused the security event(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- in response to receiving the information identifying the security event, placing the user in an elevated risk security group by causing the network device to acquire a second network address that is selected from a second subset of addresses within a second specified pool associated with

suspected malicious network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address);

wherein

- the second subset of addresses is different from the first subset of addresses(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- configuring one or more security restrictions with respect to the second network address(Col. 11, lines 23 – 34, Col. 11, lines 51 – 56, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address);

- determining whether a malicious act caused the security event(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- if a malicious act caused the security event, then providing information about the security event or malicious act to a security decision controller(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- if a malicious act did not cause the security event, then removing the user from the elevated risk group(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9).

28. The apparatus of claim 26, wherein the instructions which when executed cause the network device to acquire a second network address comprise further instructions which when executed cause:

- re-configuring a dynamic host control protocol (DHCP) server to require said server to issue any new network address to the network device only from a specified group of network addresses that is reserved for users associated with elevated user risk(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9); and

performing any one of the steps of:

(a) resetting a port that is coupled to the network device to trigger the network device to request a new network address using DHCP();

(b) issuing a DHCP FORCE_RENEW message to the network device();

(c) prompting the network device to request a new network address using DHCP(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64); or

(d) waiting for expiration of a lease for a the first network address of the network device().

30. The apparatus of claim 20, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein the instructions which when executed cause the network device to-acquire a new network address comprise instructions which when executed cause resetting a port that is coupled to the network device to prompt a user to command the network device to request a second network address using DHCP(Col. 8, lines 12 – 14, Col. 10, lines 62 - 64, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address).

31. The apparatus of claim 20, wherein

- instructions which when executed cause the network device to acquire a new network address comprise instructions which when executed cause providing the network device with an IP address that is selected from a plurality of IP addresses within a special IP subnet(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 12, lines 43 - 49).

32. The apparatus of claim 20, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein the instructions which when executed cause the network device to acquire a second network address comprise instructions which when executed cause issuing a DHCP FORCE_RENEW message to the network device(Col. 11, lines 56 - 60, the examiner further notes that the examiner

interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address).

33. The computer-readable storage medium of claim 18, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein the instructions which, when executed, cause the network device to acquire the new network address comprise instructions which when executed cause resetting a port that is coupled to the network device to prompt a user to command the network device to request a second network address using DHCP (Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 12, lines 43 - 49, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address).

34. The computer-readable storage medium of claim 18, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein the instructions which when executed cause the network device to acquire the second network address comprise instructions which when executed cause issuing a DHCP FORCE_RENEW message to the network device (Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 11, lines 56 - 60, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address,"

as the client device acquiring a new IP address).

35. The computer-readable storage medium of claim 18, wherein

- instructions which when executed cause the network device to acquire a second network address comprise instructions which when executed cause providing the network device with an IP address that is selected from a plurality of IP addresses within a special IP subnet(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 12, lines 43 - 49, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address).

36. The apparatus of claim 19, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein the means for causing the network device to acquire the second network address comprise means for resetting a port that is coupled to the network device to prompt a user to command the network device to request a new network address using DHCP(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address).

37. The apparatus of claim 19, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the second network address, and wherein

the means for causing the network device to acquire the second network address comprise means for issuing a DHCP FORCE_RENEW message to the network device(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 11, lines 56 - 60, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address).

38. The apparatus of claim 19, wherein

- the means for causing the network device to acquire a new network address comprise means for providing the network device with an IP address that is selected from a plurality of IP addresses within a special IP subnet(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64).

39. The computer-readable storage medium of claim 24, wherein the instructions which when executed cause the network device to acquire a second network address comprise further instructions which when executed cause (Col. 12, lines 43 - 59):

- re-configuring a dynamic host control protocol (DHCP) server to require said server to issue any new network address to the network device only from a specified group of network addresses that is reserved for users associated with elevated user risk (Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

and performing any one of the steps of:

(e) resetting a port that is coupled to the network device to trigger the network device to request a new network address using DHCP();

(f) issuing a DHCP FORCE_RENEW message to the network device();

(g) prompting the network device to request a new network address using DHCP(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64); or

(h) waiting for expiration of a lease for the first network address of the network device().

41. The apparatus of claim 25, wherein the means for causing the network device to acquire a second network address further comprise:

- means for re-configuring a dynamic host control protocol (DHCP) server to require said server to issue any new network address to the network device only from a specified group of network addresses that is reserved for users associated with elevated user risk(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner further notes that the examiner interprets, that the added claim limitation of, “second network address,” as the client device acquiring a

new IP address); and

means for performing any one of the steps of:

(a) resetting a port that is coupled to the network device to trigger the network device to request a new network address using DHCP();

(b) issuing a DHCP FORCE_RENEW message to the network device();

(c) prompting the network device to request a new network address using DHCP(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64); or

(d) waiting for expiration of a lease for the first network address of the network device().

43. The method of Claim 1, wherein

- causing the network device to acquire a second network address comprises performing an action that causes the network device to request a new network address(Col. 5, lines 62 - 65).

44. A method, comprising the computer-implemented steps of:

- in a security controller that is coupled, through a network, to a network device having a first network address assigned

from a first subset of addresses within a first specified pool associated with normal network users(Col.5, lines 54 – 65, the examiner notes that the security controller is either the authentication server # 310 or the DHCP server):

- in response to a security event in the network, causing the network device to acquire a second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users(Col. 5, lines 54 - 60);

wherein

- causing the network device to acquire a second network address comprises performing an action that causes the network device to request a new network address(Col. 5, lines 62 - 65);

wherein

- the second subset of addresses is different from the first subset of addresses(Col. 5, lines 62 – 65, a trusted subnet of IP addresses is different than the un-trusted subnet of IP addresses); and
- configuring one or more security restrictions with respect to the new network address(Col. 5, lines 62 – 65, the examiner notes that until the client device is authenticated, the client device is still able to utilize the network).

Thomsen does not explicitly disclose:

1. A method, comprising the computer-implemented steps of:

- in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:

- determining a user identifier associated with the network device that has caused a security event in the network;

2. A method as recited in Claim 1, further comprising the steps of:

- receiving information identifying the security event in the network;

- correlating the security event information with network user information to result in determining the user identifier associated with the network device.

9. A method as recited in Claim 1, wherein

- the step of configuring security restrictions comprises the steps of modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network

device to permit entry of IP traffic from only the second network address.

10. A method as recited in Claim 1, wherein

- the step of configuring security restrictions comprises the steps of modifying a media access control (MAC) ACL associated with a port that is coupled to the network device to permit entry of traffic only for a MAC address that is bound to the second network address.

11. A method as recited in Claim 1, further comprising

- the steps of determining whether a malicious act caused the security event, and if so, providing information about the security event or malicious act to a security decision controller.

17. A method as recited in Claim 14, wherein the step of configuring one or more security restrictions comprises the steps of:

- modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the second network address;

- and modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the second network address.

18. A computer-readable storage medium carrying one or more sequences of instructions, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

- determining a user identifier associated with the network device that has caused a security event in the network();

19. An apparatus, comprising:

- means for determining a user identifier associated with the network device that has caused a security event in the network();

20. An apparatus, comprising:

- determining a user identifier associated with the network device that has caused a security event in the network();

29. The apparatus of claim 26, wherein the instructions which when executed cause configuring one or more security restrictions comprise instructions which when executed cause:

- modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the second network address; and

- modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the second network address.

40. The computer-readable storage medium of claim 24, wherein the instructions which when executed cause configuring one or more security restrictions comprise instructions which when executed cause:

- modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the second network address; and

- modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the second network address.

42. The apparatus of claim 25, wherein the means for configuring one or more security restrictions comprise:

- means for modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the

network device to permit entry of IP traffic from only the second network address; and

- means for modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the second network address.

However, Renda discloses:

1. A method, comprising the computer-implemented steps of:

- in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users (Col. 8, lines 48 – 58, Col. 24, lines 13 - 23, Col. 25, lines 3 - 16, Col. 27, Col. 7, lines 45 - 62, lines 52 - 57, the examiner notes that the security controller is considered the master access controller or access controller):

- determining a user identifier associated with the network device that has caused a security event in the network(Col. 9, lines 45 - 55, Col. 23, lines 31 - 33, Col. 24, lines 3 - 9);

2. A method as recited in Claim 1, further comprising the steps of:

- receiving information identifying the security event in the network(Col. 7, lines 63 – 67, col. 8, lines 1 - 14);

- correlating the security event information with network user information to result in determining the user identifier associated with the network device(Col. 7, lines 63 – 67, col. 8, lines 1 - 14).

9. A method as recited in Claim 1, wherein

- the step of configuring security restrictions comprises the steps of modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the second network address(Col. 10, lines 54 - 64, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address).

10. A method as recited in Claim 1, wherein

- the step of configuring security restrictions comprises the steps of modifying a media access control (MAC) ACL associated with a port that is coupled to the network device to permit entry of traffic only for a MAC address that is bound to the second network address(Col. 10, lines 44 - 48, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address).

11. A method as recited in Claim 1, further comprising

- the steps of determining whether a malicious act caused the security event, and if so, providing information about the security event or malicious act to a security decision controller(Col. 7, lines 63 - 67, Col. 8, lines 1 - 14).

17. A method as recited in Claim 14, wherein the step of configuring one or more security restrictions comprises the steps of:

- modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the second network address(Col. 10, lines 54 - 64, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address);

- and modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the second network address(Col. 10, lines 44 - 48, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address).

18. A computer-readable storage medium carrying one or more sequences of instructions, which instructions, when executed by one or more processors, cause the one or more processors to

carry out the steps of (Col. 6, lines 4 – 18, Col. 6, lines 34 – 48):

- determining a user identifier associated with the network device that has caused a security event in the network(Col. 9, lines 45 - 55, Col. 23, lines 31 - 33, Col. 24, lines 3 - 9);

19. An apparatus, comprising:

- means for determining a user identifier associated with the network device that has caused a security event in the network(Col. 9, lines 45 - 55, Col. 23, lines 31 - 33, Col. 24, lines 3 - 9);

20. An apparatus, comprising:

- determining a user identifier associated with the network device that has caused a security event in the network(Col. 9, lines 45 - 55, Col. 23, lines 31 - 33, Col. 24, lines 3 - 9);

29. The apparatus of claim 26, wherein the instructions which when executed cause configuring one or more security restrictions comprise instructions which when executed cause:

- modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the second network address (Col. 10, lines 54 - 64, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address); and

- modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the second network address (Col. 10, lines 44 - 48, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address).

40. The computer-readable storage medium of claim 24, wherein the instructions which when executed cause configuring one or more security restrictions comprise instructions which when executed cause (Col. 6, lines 4 – 18, Col. 6, lines 34 – 48):

- modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the second network address (Col. 10, lines 54 - 64, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address); and

- modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the second network address (Col. 10, lines

44 - 48, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address).

42. The apparatus of claim 25, wherein the means for configuring one or more security restrictions comprise:

- means for modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the second network address (Col. 10, lines 54 - 64, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address); and

- means for modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the second network address (Col. 10, lines 44 - 48, the examiner further notes that the examiner interprets, that the added claim limitation of, "second network address," as the client device acquiring a new IP address).

Thomsen and Renda are analogous art because they are from the "same field of endeavor," which is the field of secure accessing of a network.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Thomsen and Renda before him or her, to modify an electronic device acquiring an internet protocol address from a pool of internet protocol addresses of known malicious user of the internet of Thomsen to include a security controller to judge whether or not the user should obtain an address from pool of internet protocol addresses that are not associated with malicious user or the user should obtain an internet address from a pool of internet protocol addresses that are associated with malicious from of Renda.

The suggestion/motivation for doing so would have been to see the abstract of Renda, also please see **KSR** v. **Teleflex**, 127 S.Ct. 1727, 1740, 82 USPQ2d 1385, 1396 (2007).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DANT B. SHAIFER HARRIMAN whose telephone number is (571)272-7910. The examiner can normally be reached on Monday - Thursday: 8:00am - 5:30pm Alt.Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

11/20/2008

/Dant B Shaifer - Harriman /
Examiner, Art Unit 2434

/ELLEN TRAN/
Primary Examiner, Art Unit 2434